(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－210025

(43)公開日　平成10年(1998)８月７日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６０１Ｅ
					６４１

審査請求　未請求　請求項の数６　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－296513

(22)出願日　平成９年(1997)10月29日

(31)優先権主張番号　特願平8－290373

(32)優先日　平８(1996)10月31日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　舘林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　福島　能久
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　中島　司朗

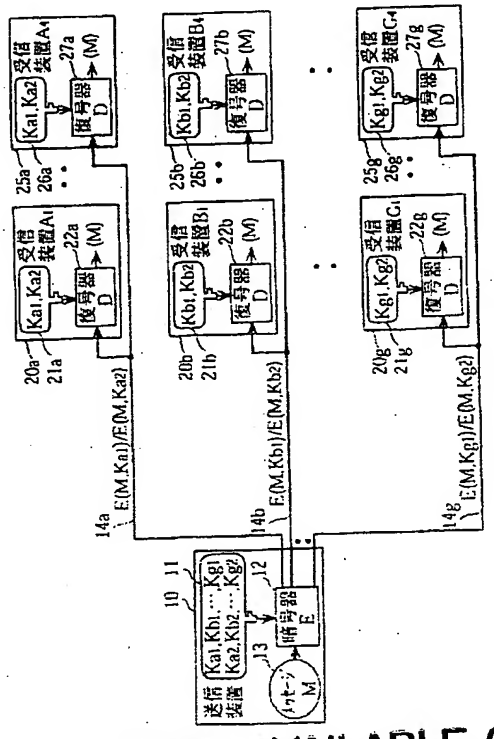
最終頁に続く

(54)【発明の名称】　暗号通信システム

(57)【要約】

【課題】　第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムを提供する。

【解決手段】　１台の送信装置１０と７つのグループＡ～Ｇに分類される合計２８台の受信装置Ａ1～Ｇ4からなる暗号通信システムにおいて、各グループには１４種類の相異なる秘密鍵から重複しないで選択した２個の秘密鍵を予め配布しておく。送信装置１０は、各グループについて配布された２個の秘密鍵のいずれかを用いて同一のメッセージＭを暗号化し、対応するグループの受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された２個の秘密鍵それぞれを用いて復号化し、得られた２個の復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。



【特許請求の範囲】
【請求項１】　ｎ台の受信装置と、それらｎ台の受信装置に対してデジタル情報を伝送する１台の送信装置とからなる暗号通信システムであって、
前記ｎ台の受信装置はｍ個のグループに分類され、各グループにはｍ×ｋ個の異なる秘密鍵から重複しないで選択されたｋ個の秘密鍵が配布されており、
前記送信装置は、
前記ｍ×ｋ個の秘密鍵と同一の秘密鍵を、配布されたグループに対応づけて予め記憶する秘密鍵記憶手段と、
前記ｍ個のグループそれぞれについて、前記秘密鍵記憶手段に記憶された各グループに対応するｋ個の秘密鍵から１個を選択して読み出す秘密鍵選択手段と、
読み出されたｍ個の秘密鍵それぞれを用いて１つの平文を暗号化する暗号化手段と、
前記暗号化手段によって得られたｍ個の暗号文を各暗号文が生成される際に用いられた秘密鍵と同一の秘密鍵を有する受信装置それぞれに伝送する伝送手段とを備え、
前記ｎ台の受信装置それぞれは、
この受信装置が属するグループに配布された前記ｋ個の秘密鍵を予め記憶する秘密鍵記憶手段と、
前記送信装置から伝送されてきた暗号文を受信する受信手段と、
受信した前記暗号文に対して前記ｋ個の秘密鍵それぞれを用いて復号化する復号手段と、
前記復号手段によって得られた復号文それぞれについて予め決められた規則性が存在するか否か判断し、少なくとも一つの復号文に規則性が存在する場合には、それら規則性が存在する復号文のひとつを前記平文と同一と認定する判断手段とを備えることを特徴とする暗号通信システム。
【請求項２】　前記送信装置の伝送手段は、前記暗号文に前記規則性を示す暗号文を添付して前記伝送を行ない、
前記受信装置の判断手段は、前記送信装置から伝送されてきた前記規則性を示す暗号文に基づいて前記判断をすることを特徴とする請求項１記載の暗号通信システム。
【請求項３】　デジタル情報をｎ台の受信装置に伝送する送信装置であって、
前記ｎ台の受信装置はｍ個のグループに分類され、各グループにはｍ×ｋ個の異なる秘密鍵から重複しないで選択されたｋ個の秘密鍵が配布され、各受信装置は自己が属するグループに配布されたｋ個の秘密鍵を有し、
前記送信装置は、
前記ｍ×ｋ個の秘密鍵と同一の秘密鍵を、配布されたグループに対応づけて予め記憶する秘密鍵記憶手段と、
前記ｍ個のグループそれぞれについて、前記秘密鍵記憶手段に記憶された各グループに対応するｋ個の秘密鍵から１個を選択して読み出す秘密鍵選択手段と、
読み出されたｍ個の秘密鍵それぞれを用いて１つの平文を暗号化する暗号化手段と、
前記暗号化手段によって得られたｍ個の暗号文を各暗号文が生成される際に用いられた秘密鍵と同一の秘密鍵を有する受信装置それぞれに伝送する伝送手段とを備えることを特徴とする送信装置。
【請求項４】　前記伝送手段は、前記暗号文に元の平文についての規則性を示す暗号文を添付して前記伝送を行なうことを特徴とする請求項３記載の送信装置。
【請求項５】　１台の送信装置から伝送されてくるデジタル情報を受信する受信装置であって、
予め配布されたｋ個の秘密鍵を記憶する秘密鍵記憶手段と、
前記ｋ個の秘密鍵のいずれかを用いて暗号化された暗号文を前記送信装置から受信する受信手段と、
受信した前記暗号文に対して前記ｋ個の秘密鍵それぞれを用いて復号化する復号手段と、
前記復号手段によって得られた復号文それぞれについて予め決められた規則性が存在するか否か判断し、少なくとも一つの復号文に規則性が存在する場合には、それら規則性が存在する復号文のひとつを正しい復号文と認定する判断手段とを備えることを特徴とする受信装置。
【請求項６】　前記受信手段は、前記暗号文と共に前記規則性を示す暗号文をも受信し、
前記判断手段は、前記規則性を示す暗号文に基づいて前記判断をすることを特徴とする請求項５記載の受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタル化された文書、音声、画像、プログラムなどのデータを伝送媒体や記録媒体を介して暗号伝送するシステムに関し、特に、１台の送信装置が秘密鍵を用いて複数の受信装置に暗号伝送する技術に関する。
【０００２】
【従来の技術】従来、ディジタル化された文書、音声、画像、プログラムなどのデータを秘密鍵で暗号化し伝送媒体を介して通信したり、記録媒体を介して記録・再生したりする秘密鍵暗号通信システムにおいては、送信装置及び受信装置それぞれは、予め装置間で定めた１個の共通の秘密鍵を用いて暗号化及び復号化を行なっている。
【０００３】つまり、送信装置及び受信装置それぞれは、複数の秘密鍵を有している場合であっても、通信を行なう直前においては、１個の秘密鍵を特定し、それを用いることとしている。これは、送信装置から送られた暗号文が受信装置において確実に復号されることを保証するためである。
【０００４】
【発明が解決しようとする課題】しかしながら、このような従来の暗号通信システムでは、通信システムの形態

が１対多、即ち、１台の送信装置が多数の受信装置に情報を提供するような形態の場合には、もし秘密鍵が解読されたときには全ての受信装置について新たな秘密鍵を設定し直さなければならず、システム構築の変更という多大な作業が強いられる。

【０００５】例えば、もし、１台の放送局と、その放送局から提供される番組を受信する１００台の受信機とが有していた秘密鍵が解読された場合には、その放送局及び１００台の受信機に記憶されている全ての秘密鍵を変更しなければならない。つまり、１台の送信装置と１台の受信装置間での通信の盗聴によって秘密鍵が解読された場合であっても、それら２台の装置だけでなく、同じ秘密鍵を共有し合う全ての受信装置に影響が及んでしまう。

【０００６】そこで、本発明は上記問題点に鑑みてなされたものであり、第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明に係る暗号通信システムは、１台の送信装置と複数のグループ化された受信装置からなる暗号通信システムであって、各グループには相異なる複数の秘密鍵から重複しないで選択した２個以上の秘密鍵を予め配布しておき、その送信装置は、各グループについて１個ずつ選択した秘密鍵それぞれを用いて１つの平文を暗号化し、得られた暗号文を対応するグループに属する受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された複数の秘密鍵それぞれを用いて復号化し、得られた復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。

【０００８】ここで、送信装置は、前記規則性を示す暗号文を前記暗号文に添付して各受信装置に送信することもできる。

【０００９】

【発明の実施の形態】

（実施の形態１）以下、本発明に係る暗号通信システムの実施の形態１について図面を用いて詳細に説明する。本暗号通信システムは、秘密鍵が解読された場合であっても、それによる被害規模を抑えることができることを特徴とする。

［暗号通信システムの概要］図１は、実施形態１に係る暗号通信システム全体のシステム構成と暗号通信の原理を説明するための図である。

【００１０】本システムは、１台の送信装置１０と、その送信装置１０から一方向で伝送される伝送情報を受信する２８台の受信装置Ａ1～G4から構成される。２８台の受信装置Ａ1～G4は、４台で１つのグループを形成する合計７つのグループＡ～Ｇのいずれかに属する。具体的には、２８台の受信装置Ａ1～G4は、バスライン１４ａに接続されたグループＡに属する４台の受信装置Ａ1～Ａ4（うち２台のみが図示されている。）、バスライン１４ｂに接続されたグループＢに属する４台の受信装置Ｂ1～Ｂ4（うち２台のみが図示されている。）、・・・、バスライン１４ｇに接続されたグループＧに属する４台の受信装置Ｇ1～Ｇ4（うち２台のみが図示されている。）からなる。

【００１１】送信装置１０は、全ての受信装置Ａ1～G4に伝えるべきメッセージ１３と、１４個の相異なる秘密鍵１１と、１個の暗号器１２とを備え、独立して接続された７本のバスライン１４ａ～１４ｇを用いることで、グループ単位、即ち、４台の受信装置ごとに、一斉同報することができる。受信装置Ａ1～G4それぞれは、２個の秘密鍵２１ａ～２１ｇ、２６ａ～２６ｇと、上記暗号器１２に対応する（逆変換をする）１個の復号器２２ａ～２２ｇ、２７ａ～２７ｇとを備える。

【００１２】本システムの目的は、秘密鍵を用いた暗号通信により、１台の送信装置１０が２８台の受信装置Ａ1～G4に対して１つの（同一の）メッセージＭを伝えることである。まず、送信装置１０が備える１４個の秘密鍵１１と各受信装置が備える２個の秘密鍵との関係（秘密鍵の配布形態）を説明する。

【００１３】７つのグループＡ～Ｇそれぞれには、相異なる１４種類の秘密鍵の中から重複しないで選択した２個の秘密鍵を予め配布しておく。つまり、グループＡには秘密鍵Ｋa1及びＫa2を配布し、グループＢには秘密鍵Ｋb1及びＫb2を配布し、・・・、グループＧには秘密鍵Ｋg1及びＫg2を配布しておく。そして、各受信装置Ａ1～G4それぞれは、自己が属するグループに配布された２個の秘密鍵を記憶しておく。

【００１４】一方、送信装置１０は、７つのグループＡ～Ｇに配布されたものと同一の１４個の秘密鍵を各グループに対応づけて記憶しておく。このようにして、１４個の秘密鍵は、同一のグループに属する受信装置間では共通化され、異なるグループに属する受信装置間では、共通化されないようにしている。

【００１５】次に、送信装置１０が２８台の受信装置Ａ1～G4に伝送する具体的な暗号文の内容を説明する。送信装置１０が２８台の受信装置Ａ1～G4に伝送する暗号文は、本図のバスライン１４ａ～１４ｇに示されている通りである。ここで、記号Ｅ（Ｍ，Ｋ）は、平文Ｍに対して暗号鍵Ｋを用いて暗号アルゴリズムＥに基づいて暗号化して得られた暗号文を意味する。同様に、記号Ｄ（Ｃ，Ｋ）は、暗号文Ｃに対して復号鍵Ｋを用いて復号アルゴリズムＤに基づいて復号化して得られた復号文を意味する。

【００１６】すなわち、送信装置１０は、バスライン１４ａを介してグループＡに属する４台の受信装置Ａ1～

A4に対しては暗号文E（M，Ka1）又はE（M，Ka2）（本図では、E（M，Ka1）／E（M，Ka2）と記されている）を伝送し、バスライン１４ｂを介してグループBに属する４台の受信装置B1～B4に対しては暗号文E（M，Kb1）又はE（M，Kb2）を伝送し、・・、バスライン-１４ｇを介してグループGに属する４台の受信装置G1～G4に対しては暗号文E（M，Kg1）又はE（M，Kg2）を伝送する。

【００１７】具体的には、送信装置１０は、グループAに対しては、グループAに配布された２個の秘密鍵（Ka1及びKa2）のいずれかをランダムに選択し、それを用いてメッセージMを暗号器１２で暗号化し、得られた暗号文E（M，Ka1）又はE（M，Ka2）をグループAに属する４台の受信装置A1～A4に一斉同報する。同様に、グループBに対しては、グループBに配布された２個の秘密鍵（Kb1及びKb2）のいずれかを選択し、それを用いてメッセージMを暗号器１２で暗号化し、得られた暗号文E（M，Kb1）又はE（M，Kb2）をグループBに属する４台の受信装置B1～B4に一斉同報する。このようにして、グループごとに異なる暗号文を順次、一斉同報していく。

【００１８】一方、受信装置A1～G4それぞれは、受信した暗号文に対して自己が保有する２個の秘密鍵それぞれを用いて復号化し、得られた２種類の復号文の少なくとも１つが信頼できる内容であるならば、その復号文は送信装置１０が伝えてきたメッセージMであり、かつ、その復号文を得るために用いた秘密鍵は送信装置１０が用いたものと同一と認定する。

【００１９】具体的には、受信装置２０ａであれば、受信した暗号文（E（M，Ka1）又はE（M，Ka2））に対して、秘密鍵Ka1及びKa2それぞれを用いて復号化し、得られた２個の復号文について、少なくとも１つが信頼できるか否かを、その内容に一定の規則性が存在するか否かで判断する。なお、「一定の規則性」の具体的基準は後述する。

【００２０】以上のように、本暗号通信システムによって、１つのメッセージMが１台の送信装置１０から２８台の受信装置２０ａに秘密伝送されたが、このシステムには大きく２つの特徴がある。第１に、異なるグループに属する受信装置間では、秘密鍵が共通化されていないことである。

【００２１】従って、もし、１つのグループに配布された秘密鍵が不正者によって解読された場合であっても、他のグループに属する受信装置は影響を受けない、即ち、秘密鍵の変更を強いられないという利点がある。第２に、１つのグループには２個の秘密鍵が配布されているが、実際に用いられる秘密鍵は、それらから選択された１個のみである。

【００２２】従って、もし、その１個の秘密鍵が不正者によって解読された場合であっても、以降の伝送においては残る１個の秘密鍵を採用することにより、たとえ同一グループに属する受信装置であっても、秘密鍵を入れ替えることなく秘密通信を継続していくことができる。

［具体的な構成］図２は、図１に示された暗号通信システムにおける送信装置１０と１台の受信装置２０ａのみに着目し、それらの詳細な構成を示すブロック図である。

【００２３】送信装置１００は、図１における送信装置１０に相当し、デジタル著作物１０１、秘密鍵記憶部１０３、秘密鍵選択部１０４、３個の暗号器１０２、１０５、１０７、メッセージ生成部１０６及び３個の送信部１１０～１１２から構成される。この送信装置１００は、自己が保有するデジタル著作物を暗号化して受信装置A1に転送することを最終的な目的とし、そのために、暗号化されたデジタル著作物Cdの他に、２種類の暗号文、即ち、そのデジタル著作物の暗号化に用いた１個の秘密鍵を暗に伝えるための暗号文Caと、その秘密鍵を特定するための判断基準となる一定の規則性を伝えるための暗号文Cmとを併せて受信装置A1に送信する。

【００２４】デジタル著作物１０１は、デジタル化された文書、音声、画像、プログラムなどのデータを予め保持しているハードディスク等である。秘密鍵記憶部１０３は、図１における秘密鍵１１に相当し、全てのグループA～Gに配布されたものと同一の１４個の秘密鍵を、配布されたグループに対応づけて予め記憶する半導体メモリ等である。

【００２５】秘密鍵選択部１０４は、上記３つの暗号文の生成・送信に先立ち、送信先となる受信装置が属するグループに対応する２個の秘密鍵のいずれかをランダムに選択して秘密鍵記憶部１０３から読み出し、それを２個の暗号器１０２及び１０５それぞれに伝える。具体的には、送信先が受信装置A1の場合には、秘密鍵Ka1又はKa2を選択して秘密鍵記憶部１０３から読み出し、暗号器１０２及び１０５に送る。

【００２６】暗号器１０２は、秘密の暗号アルゴリズムE1に基づく暗号化をするＩＣ等であり、デジタル著作物１０１からブロック単位でデジタルデータDataを読み出し、それに対して秘密鍵選択部１０４から送られてきた秘密鍵Ka1又はKa2で暗号化し、得られた暗号文Cd（＝E1（Data，Ka1）／E1（Data，Ka2））を送信部１１０に送るという処理をデジタル著作物１０１全てについて繰り返す。

【００２７】メッセージ生成部１０６は、図１におけるメッセージ１３に相当し、送信先のグループが異なるごとに新たな１個の乱数を発生し、メッセージMとして保持する乱数発生器等である。なお、本実施形態においては、メッセージMは、上記デジタル著作物１０１の暗号化に用いた秘密鍵を受信装置A1に伝達するためのキャリアとして用いられるダミーデータであり、その内容は重要でない。

【００２８】暗号器１０５は、秘密の暗号アルゴリズムE2に基づく暗号化をするＩＣ等であり、メッセージ生成部１０６に保持されたメッセージMを読み出し、それに対して秘密鍵選択部１０４から送られてきた秘密鍵Ka1又はKa2で暗号化し、得られた暗号文Ca（＝E2（M，Ka1）／E2（M，Ka2））を送信部１１１に送る。

【００２９】暗号器１０７は、秘密の暗号アルゴリズムE3に基づく暗号化をするＩＣ等であり、メッセージ生成部１０６に保持されたメッセージMを読み出し、そのメッセージMに対してそのメッセージMを暗号鍵として暗号化し、得られた暗号文Cm（＝E3（M，M））を送信部１１２に送る。送信部１１０、１１１、１１２は、並列to直列変換器や増幅器等からなり、それぞれ、バスライン１２０、１２１、１２２を介して上記３種類の暗号文Cd、Ca、Cmを受信装置A1に送信する。なお、３本のバスライン１２０～１２２をまとめたものが図１における１本のバスライン14ａに相当する。

【００３０】一方、受信装置A1は、図１における受信装置２０ａに相当し、５個の復号器２０１、２２１、２２２、２３１、２３２、２個の秘密鍵記憶部２２０、２３０、２個の判定部２２３、２３３、総合判定部２０３、秘密鍵選択部２０２、３個の受信部２１０～２１２から構成される。この受信装置A1は、送信装置１００から送られてきた暗号化デジタル著作物Cdを復号化して利用することを最終的な目的とし、その復号のために用いるべき秘密鍵、即ち、送信装置１００が用いた秘密鍵は、暗号化デジタル著作物Cdと共に受信した２種類の暗号文Ca及びCmから特定する。

【００３１】受信部２１０、２１１、２１２は、直列to並列変換器等からなり、それぞれ、バスライン１２０、１２１、１２２を介して上記３種類の暗号文Cd、Ca、Cmを受信する。復号器２０１は、送信装置１００が備える暗号器１０２の暗号アルゴリズムE1の逆変換である秘密の復号アルゴリズムD1に基づく復号化をするＩＣ等であり、秘密鍵選択部２０２から秘密鍵Ka1又はKa2が与えられた場合には、受信部２１０から送られてきた暗号文Cdに対して、その秘密鍵を用いて復号化することにより、元のデジタル著作物のブロックデータDataに復元する。

【００３２】なお、この復号器２０１は、送信装置１００から繰り返し暗号化デジタル著作物Cdが送られてくる限り、その復号化を繰り返す。また、秘密鍵選択部２０２から秘密鍵が与えられない場合には、秘密鍵の特定に失敗したものと認識し、暗号化デジタル著作物Cdの復号化は行なわない。秘密鍵記憶部２２０、復号器２２１、復号器２２２及び判定部２２３からなる１組の回路群は、送信装置１００で用いられた秘密鍵がKa1であるか否かを判定することを目的とし、一方、秘密鍵記憶部２３０、復号器２３１、復号器２３２及び判定部２３３からなる他の１組の回路群は、送信装置１００で用いられた秘密鍵がKa2であるか否かを判定することを目的とする。これら２組の回路群は、秘密鍵記憶部２２０及び２３０に記憶された１個の秘密鍵が異なる点を除いて基本的な構成及び機能は同一である。従って、一方の組のみ詳述する。

【００３３】秘密鍵記憶部２２０は、図１における秘密鍵２１ａに相当し、秘密鍵Ka1を予め記憶する半導体メモリ等である。復号器２２１は、送信装置１００が備える暗号器１０５の暗号アルゴリズムE2の逆変換である秘密の復号アルゴリズムD2に基づく復号化をするＩＣ等であり、図１における復号器２２ａに相当し、受信部２１１から送られてきた暗号文Caに対して秘密鍵記憶部２２０から読み出した秘密鍵Ka1を用いて復号化し、得られた復号文M1（＝D2（Ca，Ka1））を判定部２２３及び復号器２２２に送る。

【００３４】復号器２２２は、送信装置１００が備える暗号器１０７の暗号アルゴリズムE3の逆変換である秘密の復号アルゴリズムD3に基づく復号化をするＩＣ等であり、受信部２１２から送られてきた暗号文Cmに対して復号器２２１から送られてきた復号文M1を復号鍵として復号化し、得られた復号文M11（＝D3（Cm，M1））を判定部２２３に送る。

【００３５】判定部２２３は、比較器及びセレクタ等からなり、復号器２２１から送られてきた復号文M1と復号器２２２から送られてきた復号文M11とが一致するか否かを判定し、一致する場合にはその復号文M1を、一致しない場合には「０」を、総合判定部２０３に出力する。ここで、一致する場合（M1＝M11）とは、送信装置１００において選択され用いられた秘密鍵がKa1である場合に相当する。その理由は、以下の通りである。

【００３６】いま、送信装置１００において、秘密鍵選択部１０４は秘密鍵Ka1を選択したとする。すると、以下が成立する。

Ca＝E2（M，Ka1）　　－式１

Cm＝E3（M，M）　　－式２

よって、受信装置A1の復号器２２１が出力する復号文M1は、式１を用いることにより、以下の通りとなる。

【００３７】

M1＝D2（Ca，Ka1）

＝D2（E2（M，Ka1），Ka1）

＝M　　－式３

一方、受信装置A1の復号器２２２が出力する復号文M11は、式２と式３を用いることにより、以下の通りとなる。

【００３８】

M11＝D3（Cm，M1）

＝D3（E3（M，M），M）

＝M　　－式４

よって、式３と式４とから、以下が成立する。

M1＝M11　　－式５

なお、同様にして、もう１組の回路群の判定部２３３は、復号器２３１から送られてきた復号文M2と復号器２３２から送られてきた復号文M22とが一致するか否かを判定し、一致する場合にはその復号文M2を、一致しない場合には「０」を、総合判定部２０３に出力する。

【００３９】総合判定部２０３は、論理和回路及びセレクタ等からなり、判定部２２３及び判定部２３３から出力された復号文に基づいて、受信した暗号化デジタル著作物Cdの復号化に用いるべき復号鍵（Ka1及びKa2のいずれか）を特定する指示を、又は、復号鍵が見当たらない旨の指示を秘密鍵選択部２０２に送る。具体的には、判定部２２３が「０」でない復号文M2を出力した場合には判定部２３３の出力いかんに拘わらず秘密鍵Ka1を選択する指示「１」を、判定部２２３が「０」を出力し、かつ、判定部２３３が「０」でない復号文M2を出力した場合には秘密鍵Ka2を選択する指示「２」を、その他の場合には復号鍵が見当たらない旨の指示「０」を、それぞれ秘密鍵選択部２０２に送る。

【００４０】秘密鍵選択部２０２は、セレクタ等からなり、総合判定部２０３からの３種類の指示「０／１／２」に基づいて、それぞれ、復号器２０１に秘密鍵を出力しない／秘密鍵Ka1を出力する／秘密鍵Ka2を出力する。秘密鍵選択部２０２は、送信装置１００から暗号化デジタル著作物Cdが繰り返し送信されてくる間、その出力を継続する。

【００４１】なお、判定部２２３（２３３）は復号文M1（M2）と復号文M11（M22）とが一致しない場合に「０」を出力し、その結果、総合判定部２０３は、その不一致に係る秘密鍵Ka1（Ka2）は送信装置１００において選択された秘密鍵ではないとして上記処理をしているが、これは、本システムに採用されているような暗号（復号）アルゴリズムが通常持つ以下の性質を利用している。

【００４２】つまり、「暗号文に対して本来用いるべき秘密鍵とは異なる秘密鍵を復号鍵として復号化した場合に得られる復号文は、元の平文とは異なる。」という性質である。

［暗号通信システムの動作］次に、以上のように構成された本暗号通信システムの動作を説明する。

【００４３】図３は、送信装置１００の動作手順を示すフローチャートである。送信装置１００は、７つのグループA～Gそれぞれについて以下の処理（ステップS５１～S５３）を繰り返す（ステップS５０～S５４）。なお、ステップS５１～S５３に記入されてる記号・式は、グループAに対する処理の場合におけるものであり、以下、その場合のみについて説明する。

【００４４】まず、秘密鍵選択部１０４は、グループAに対応する２個の秘密鍵Ka1及びKa2からランダムに１個を選択し、暗号器１０２及び暗号器１０５に送る（ステップS５１）。次に、暗号器１０２は上記ステップS５１で選択された１個の秘密鍵Ka1／Ka2を用いてデジタル著作物１０１のブロックデータDataを暗号化することにより暗号文Cdを生成し、暗号器１０５は同じ１個の秘密鍵Ka1／Ka2を用いてメッセージ生成部１０６で生成されたメッセージMを暗号化することにより暗号文Caを生成し、暗号器１０７は同じメッセージMを暗号鍵としてそのメッセージMを暗号化することにより暗号文Cmを生成する（ステップS５２）。これら３つの暗号化は同時並列に行われる。

【００４５】最後に、３つの送信部１１０、１１１、１１２それぞれは、上記ステップS５２で得られた３つの暗号文Cd、Ca、Cmそれぞれをバスライン１２０、１２１、１２２それぞれを介してグループAに属する４台の受信装置A1～A4に一斉同報する（ステップS５４）。このようにしてグループAに対する送信が終了すると、送信装置１００は、次にグループBに対しても同様の送信処理を行うというように、順次７つのグループA～G全てに対して同様の処理を繰り返していく（ステップS５０～S５４）。

【００４６】図４は、受信装置A1の動作手順を示すフローチャートである。なお、他の受信装置A2～G4の動作手順も基本的には本図と同じである。まず、受信部２１０、２１１、２１２は、それぞれ、送信装置１００からバスライン１２０、１２１、１２２を介して送られてきた３つの暗号文Cd、Ca、Cmを受信し、復号器２０１、復号器２２１及び復号器２３１、復号器２２２及び復号器２３２に送る（ステップS６０）。

【００４７】次に、第１段階の復号化として、受信部２１１から送られてきた暗号文Caに対して、復号器２２１は秘密鍵記憶部２２０から読み出した秘密鍵Ka1を用いて復号化することにより復号文M1を生成すると同時に、復号器２３１は秘密鍵記憶部２３０から読み出した秘密鍵Ka2を用いて復号化することにより復号文M2を生成する（ステップS６１）。

【００４８】続いて、第２段階の復号化として、受信部２１２から送られてきた暗号文Cmに対して、復号器２２２は復号器２２１が生成した復号文M1を復号鍵として用いて復号化することにより復号文M11を生成し、これと同時並列に、復号器２３２は復号器２３１が生成した復号文M2を復号鍵として用いて復号化することにより復号文M22を生成する（ステップS６２）。

【００４９】そして、判定部２２３は復号器２２１が生成した復号文M1と復号器２２２が生成した復号文M11とが一致するか否かを判定し、一致する場合には復号文M1を、一致しない場合には「０」を総合判定部２０３に出力し、これと同時並列に、判定部２３３は復号器２３１が生成した復号文M2と復号器２３２が生成した復号文M22とが一致するか否かを判定し、一致する場合には復号文M2を、一致しない場合には「０」を総合判定

部２０３に出力する（ステップＳ６３、Ｓ６４）。

【００５０】その結果、判定部２２３から一致した旨の通知（復号文M1）を受けた場合には、総合判定部２０３は、その通知を判定部２３３からの通知に優先させ、秘密鍵選択部２０２に対して秘密鍵Ka1を選択する旨の指示「１」を送る。従って、復号器２０１は、受信部２１０から送られてきた暗号文Cdに対して秘密鍵選択部２０２から送られてきた秘密鍵Ka1を用いて元のデジタル著作物Dataに復号化する（ステップＳ６５）。

【００５１】一方、判定部２２３から一致しない旨の通知（「０」）を受けた場合には、総合判定部２０３は、さらに判定部２３３から受けた通知内容を判断し、その結果、一致した旨の通知（復号文M2）であるときには、秘密鍵選択部２０２に対して秘密鍵Ka2を選択する旨の指示「２」を送る。従って、復号器２０１は、受信部２１０から送られてきた暗号文Cdに対して秘密鍵選択部２０２から送られてきた秘密鍵Ka2を用いて元のデジタル著作物Dataに復号化する（ステップＳ６６）。

【００５２】判定部２２３及び判定部２３３のいずれからも一致しない旨の通知（「０」）を受けた場合には、総合判定部２０３は、秘密鍵選択部２０２に対してその旨の通知「０」を送る。従って、復号器２０１は、受信部２１０から送られてきた暗号文Cdに対して復号化を行なわない（ステップＳ６６）。以上のように、本実施形態によれば、７つのグループそれぞれに１４種類の相異なる秘密鍵から重複しないで選択した２個の秘密鍵を予め配布しておき、送信装置１００は、各グループにつき任意に選択した１個の秘密鍵を用いて暗号化することで、デジタル著作物１０１及びメッセージMを秘密にして２８台の受信装置A1～E4に伝達することができる。

【００５３】この方式によれば、例えば、バスライン１４ａを繰り返し盗聴することで１個の秘密鍵Ka1が不正者に解読された場合であっても、他のグループＢ～Ｇに属する受信装置は、その秘密鍵Ka1と異なる秘密鍵を用いているので、それによる影響を受けることなく通信を継続することができる。さらに、送信装置１０は、解読された秘密鍵Ka1を用いることなく、残る秘密鍵Ka2を用いることで、グループＡに属する受信装置との通信を継続することができる。

【００５４】つまり、１個の秘密鍵が漏洩したり解読された場合であっても、送信装置及び全ての受信装置は、新たな秘密鍵の配布を受けて記憶したり、記憶すべき秘密鍵を更新したりすることなく、秘密通信を継続することができる。以上、本発明に係る暗号通信システムについて、実施形態に基づいて説明したが、本発明はこれら実施形態に限られないことは勿論である。即ち、

（１）本実施形態では、暗号通信システムのネットワーク形態はスター型であり、１台の送信装置が各受信装置ごとに異なる暗号文を送信したが、本発明は、このようなネットワーク形態に限らない。１本の同軸ケーブルに送信装置及び全ての受信装置が接続されたバス型のネットワークであって、１台の送信装置が複数の受信装置に対して全ての受信装置向けの暗号文をまとめて一斉同報してもよい。

（２）また、本暗号通信システムにおける通信媒体は有線のバスライン１４ａ～１４ｇであったが、ＣＤ－ＲＯＭ等の記録媒体であってもよい。

【００５５】図5は、本発明に係る暗号通信システムの通信媒体がＣＤ－ＲＯＭ２５０である場合における、送信装置によって書き込まれたＣＤ－ＲＯＭ２５０の内容を示す図である。送信装置（ＣＤ－ＲＯＭライタ）は、各グループに対応して予め定められた７つの記録位置２５１～２５７それぞれに、各グループ充てに送信する３つの暗号文Cd２５８、Ca２５９、Cm２６０を記録しておき、一方、受信装置（ＣＤ－ＲＯＭドライブ）は、自己が属するグループに対応する記録位置に記録された３つの暗号文Cd２５８、Ca２５９、Cm２６０を読み出し、デジタル著作物Dataに復号化する、という暗号通信システムであってもよい。

（３）また、本実施形態では、３種類の異なる暗号アルゴリズムが用いられたが、これらは同一であってもよい。さらに、複数の秘密鍵記憶部や複数の暗号器・復号器を１個の半導体ＩＣに形成された回路で実現してもよい。

（４）また、本実施形態では、秘密鍵選択部１０４はランダムに秘密鍵を選択したが、このような選択方式に限られず、例えば、予め定めらた優先順位に従って秘密鍵を選択し、もしその秘密鍵が解読された場合に他の秘密鍵を選択することとしてもよい。

（５）また、本実施形態では、各グループに２個ずつ秘密鍵が配布され、それらから選択された１個だけが暗号化に用いられたが、このような数値に限定されない。例えば、送信装置１００は、各グループについて配布された４個の秘密鍵から選択した３個の秘密鍵を結合したもの（例えばビットごとの排他的論理和をとったもの）を暗号鍵として暗号文を生成し、各受信装置は、その暗号文に対して、４個の秘密鍵から選択可能な３個の秘密鍵の組み合わせ全てについてそれら３個の秘密鍵のビットごとの排他的論和によって得られるものを復号鍵としてそれぞれ復号化することで本実施形態と同じ判定を行い、少なくとも１組の復号鍵について上述の２つの復号文Mn及びMnnが一致した場合に、その一致に係る秘密鍵の組合せが送信装置１００で選択されたものと判断すればよい。

（６）さらに、本実施形態では、２台以上の受信装置によって１つのグループが形成されたが、各グループに属する受信装置は１台であってもよい。つまり、受信装置ごとに異なる２個以上の秘密鍵を配布しておき、送信装置は、受信装置ごとに異なる秘密鍵を用いた暗号文を送信してもよい。

（実施の形態２）次に、本発明に係る暗号通信システムの実施の形態２について図面を用いて詳細に説明する。本暗号通信システムは、３階層の暗号化を行うことを特徴とする。

［暗号通信システムの構成］図６は、実施形態２に係る暗号通信システム全体のシステム構成と暗号通信の原理を説明するための図である。

【００５６】本システムは、３階層の暗号化によってデジタル著作物等の著作権を保護せんとする暗号通信システムであり、ＤＶＤ（Digital Video/Versatile Disc）３１０用の記録装置３００と再生装置３２０とから構成される。記録装置３００は、デジタルデータをＤＶＤ３１０に記録する装置であり、マスター鍵（Ｋｍ）記憶部３０１と、媒体鍵（Ｋｄ）生成部３０２と、タイトル鍵（Ｋｔ）生成部３０３と、３種類の暗号器３０５～３０７と、文書、画像、音声等のデジタルデータを記憶するデジタル著作物３０４とを備える。

【００５７】マスター鍵記憶部３０１は、マスター鍵Ｋｍ、即ち、正規の（再生が許可された）再生装置３２０と共有し合う秘密鍵を予め保持し、媒体鍵生成部３０２は、媒体鍵Ｋｄ、即ち、個々のＤＶＤ３１０を区別するための秘密鍵を生成し、タイトル鍵生成部３０３は、タイトル鍵Ｋｔ、即ち、ＤＶＤ３１０に記録するデジタル著作物３０４のタイトル（例えば１本の映画）ごとに付与する秘密鍵を生成する。

【００５８】３個の暗号器３０５～３０７は、それぞれ、異なる秘密の暗号アルゴリズムＥ1、Ｅ2、Ｅ3に基づいて、媒体鍵Ｋｄ、タイトル鍵Ｋｔ、デジタル著作物Ｄａｔａを暗号化し、それぞれ暗号化媒体鍵３１１、暗号化タイトル鍵３１２、暗号化デジタル著作物３１３を生成する。再生装置３２０は、記録装置３００によって記録されたＤＶＤ３１０の暗号化デジタル著作物３１３を読み出して復号化する正規の装置であり、記録装置３００が備えるマスター鍵記憶部３０１と同一のマスター鍵Ｋｍを記憶するマスター鍵Ｋｍ記憶部３２１と、３個の復号器３２２～３２４とを備える。

【００５９】３個の復号器３２２～３２４は、それぞれ、記録装置３００が備える暗号器３０５、３０６、３０７の暗号アルゴリズムＥ1、Ｅ2、Ｅ3の逆変換である秘密の復号アルゴリズムＤ1、Ｄ2、Ｄ3に基づいて、ＤＶＤ３１０から読み出された暗号化媒体鍵３１１、暗号化タイトル鍵３１２、暗号化デジタル著作物３１３を復号化する。

［暗号通信システムの動作］以上のように構成された本暗号通信システムの動作について図６に従って説明する。

【００６０】記録装置３００においては、以下の３階層の暗号化が行われる。つまり、暗号器３０５はマスター鍵記憶部３０１から読み出したマスター鍵Ｋｍを暗号鍵として媒体鍵生成部３０２で生成された媒体鍵Ｋｄを暗号化することで暗号化媒体鍵Ｅ1（Ｋｄ、Ｋｍ）３１１を生成し、暗号器３０６はその媒体鍵Ｋｄを暗号鍵としてタイトル鍵生成部３０３で生成されたタイトル鍵Ｋｔを暗号化することで暗号化タイトル鍵Ｅ2（Ｋｔ、Ｋｄ）３１２を生成し、暗号器３０７はそのタイトル鍵Ｋｔを暗号鍵としてデジタル著作物Ｄａｔａ３０４を暗号化することで暗号化デジタル著作物Ｅ3（Ｄａｔａ、Ｋｔ）３１３を生成する。

【００６１】生成された暗号化媒体鍵Ｅ1（Ｋｄ、Ｋｍ）３１１、暗号化タイトル鍵Ｅ2（Ｋｔ、Ｋｄ）３１２、暗号化デジタル著作物Ｅ3（Ｄａｔａ、Ｋｔ）３１３は、記録装置３００によってＤＶＤ３１０の所定箇所に記録される。一方、再生装置３２０においては、以下の３階層の復号化が行われる。つまり、ＤＶＤ３１０に記録された暗号化媒体鍵Ｅ1（Ｋｄ、Ｋｍ）３１１、暗号化タイトル鍵Ｅ2（Ｋｔ、Ｋｄ）３１２、暗号化デジタル著作物Ｅ3（Ｄａｔａ、Ｋｔ）３１３が再生装置３２０によって読み出された後に、まず、復号器３２２はマスター鍵Ｋｍ記憶部３２１から読み出したマスター鍵Ｋｍを復号鍵として暗号化媒体鍵Ｅ1（Ｋｄ、Ｋｍ）３１１を復号化することで媒体鍵Ｋｄを生成する。これは、以下の式６より明らかである。

【００６２】

Ｋｄ＝Ｄ1（Ｅ1（Ｋｄ、Ｋｍ）、Ｋｍ）　　－式６

続いて、復号器３２３は、復号器３２２によって生成された媒体鍵Ｋｄを復号鍵として暗号化タイトル鍵Ｅ2（Ｋｔ、Ｋｄ）３１２を復号化することでタイトル鍵Ｋｔを生成する。これは、以下の式７より明らかである。

Ｋｔ＝Ｄ2（Ｅ2（Ｋｔ、Ｋｄ）、Ｋｄ）　　－式７

最後に、復号器３２４は、復号器３２３によって生成されたタイトル鍵Ｋｔを復号鍵として暗号化デジタル著作物Ｅ3（Ｄａｔａ、Ｋｔ）３１３を復号化することでデジタル著作物Ｄａｔａを生成する。これは、以下の式８より明らかである。

【００６３】

Ｄａｔａ＝Ｄ3（Ｅ3（Ｄａｔａ、Ｋｔ）、Ｋｔ）　　－式８

ここで、もし、再生装置３２０が備えるマスター鍵Ｋｍが記録装置３００が備えるマスター鍵Ｋｍと一致しないものである場合には、復号器３２２から生成された鍵は、もはや記録装置３００が備えるタイトル鍵Ｋｔと一致しなくなる。従って、残る２階層の復号化が行われても、復号器３２４から出力されるデータは、元のデジタル著作物Ｄａｔａ３０４とは一致しない。

【００６４】つまり、記録装置３００が備えるマスター鍵Ｋｍと同じマスター鍵を備える再生装置３２０だけが元のデジタル著作物３０４を得ることができる。以上のように、本暗号通信システムによれば、ＤＶＤ３１０にはデジタル著作物３０４が暗号化されて記録されており、その暗号化デジタル著作物３１３を読み出して復号できるのは、マスター鍵Ｋｍを備える再生装置３２０に

限定される。そして、DVD３１０には更にDVD３１０ごとに固有の媒体鍵Kd及びデジタル著作物３０４のタイトルごとに固有のタイトル鍵Ktが暗号化されて記録されており、これらを順次に復号化することに成功して初めて特定のタイトルに係るデジタル著作物Dataの復号化に成功する。

【００６５】つまり、記録媒体に全ての暗号鍵が保存されることによる暗号鍵の漏洩やデッドコピー等の不具合・不正が防止されると共に、コンテンツの再生が許可された再生装置とそうでないものとの区別を設ける等の管理が容易となる。

（実施の形態３）次に、本発明に係る暗号化装置の実施の形態３について図面を用いて詳細に説明する。本暗号装置は、秘密鍵をそのまま用いるのではなく、修正を加えて得られる修正秘密鍵を用いて暗号化することを特徴とする。

［暗号化装置の構成］図７は、実施形態３に係る暗号化装置４００の構成を示すブロック図である。

【００６６】暗号化装置４００は、デジタル著作物４０２を暗号化して送信する装置であり、タイトル鍵Kt生成部４０１、デジタル著作物４０２、修正部４０３、分離部４０４、暗号器４０５及び結合部４０６を備える。タイトル鍵Kt生成部４０１、デジタル著作物４０２及び暗号器４０５は、実施形態２におけるタイトル鍵生成部３０３、デジタル著作物３０４及び暗号器３０７と同一である。

【００６７】分離部４０４は、ラッチ回路等からなり、デジタル著作物４０２から取り出したブロックデータDataのうち、暗号化しない部分（分離データData１）と暗号化する部分（分離データData2）とに分離し、前者を修正部４０３及び結合部４０６に送り、後者を暗号器４０５に送る。修正部４０３は、排他的論理和回路等からなり、タイトル鍵Kt生成部４０１で生成されたタイトル鍵Ktと、分離部４０４から送られてきた分離データData1とのビットごとの排他的論理和を算出し、その結果得られたものを以下の式９に示される修正タイトル鍵Kpとして暗号器４０５に送る。

【００６８】Kp＝Kt(+)Data1　　－式９

なお、記号(+)は、排他的論理和を示す演算子である。

暗号器４０５は、修正部４０３から送られてきた修正タイトル鍵Kpを暗号鍵とし分離部４０４から送られてきた分離データData2を秘密の暗号アルゴリズムＥに基づいて暗号化し、得られた暗号文Ｅ（Data2、Ｋp）を結合部４０６に送る。この暗号文Ｅ（Data2、Kp）は、上記式９より、以下の式１０の如く表現される。

【００６９】

E（Data2、Kp）＝E（Data2、Kt(+)Data1）　　－式１０

結合部４０６は、ラッチ回路等からなり、分離部４０４から送られてきた分離データData1と、暗号器４０５から送られてきた暗号文Ｅ（Data2、Kp）とを結合することで、元のブロックデータDataに対応する暗号化ブロックデータEdataを出力する。

【００７０】図８は、暗号化される前のブロックデータData及び暗号化された後のブロックデータＥdataの構造を示す図である。分離データData1はそのまま変化しないが、分離データData2は、分離データData1によって修正されたタイトル鍵Kpで暗号化される。以上のように、本暗号化装置４００によれば、秘密鍵は、そのまま暗号鍵として用いられるのではなく、修正を受けた後に用いられる。そして、その修正内容は、暗号化の対象となるデジタル著作物の一部が用いられる。

【００７１】これによって、最終的な暗号鍵はコンテンツに依存して決定されることになり、不正な第３者による秘密鍵の推定を困難にすると共に、秘密鍵だけが漏洩することによって他の全てのコンテンツが解読されてしまうという最悪自体の発生も回避される。

【００７２】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号通信システムは、１台の送信装置と複数のグループ化された受信装置からなる暗号通信システムであって、各グループには相異なる複数の秘密鍵から重複しないで選択した２個以上の秘密鍵を予め配布しておき、その送信装置は、各グループについて１個ずつ選択した秘密鍵それぞれを用いて１つの平文を暗号化し、得られた暗号文を対応するグループに属する受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された複数の秘密鍵それぞれを用いて復号化し、得られた復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。

【００７３】これにより、もし１個の秘密鍵が解読された場合であっても、その秘密鍵が配布されたグループとは異なるグループについての暗号通信は影響を受けることなく継続することができる。また、解読された秘密鍵が配布されたグループについては、残る他の秘密鍵を用いて暗号通信を継続することも可能である。さらに、送信装置は各グループについて用いる秘密鍵を任意に変更することができるので、繰り返し同じ秘密鍵を用いることが回避され、第三者による秘密鍵の解読は困難となる。

【００７４】つまり、第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムが実現される。ここで、送信装置は、前記規則性を示す暗号文を前記暗号文に添付して各受信装置に送信してもよい。

【００７５】これによって、受信装置が複数の復号文の中から正しいものを特定する際の判断基準は暗号化されて送信装置から受信装置に伝送されるので、送信装置が

選択した1個の秘密鍵がいずれであるかという情報も隠ぺいされ、安全性の高い暗号通信が実現される。

【図面の簡単な説明】

【図1】本発明の実施形態1に係る暗号通信システム全体の構成と暗号通信の原理を説明するための図である。

【図2】同暗号通信システムにおける送信装置10と1台の受信装置20aについての詳細な接続と構成を示すブロック図である。

【図3】送信装置100の動作手順を示すフローチャートである。

【図4】受信装置A1の動作手順を示すフローチャートである。

【図5】本発明に係る暗号通信システムの通信媒体が記録媒体である場合における、その記録媒体に書き込まれる内容を示す図である。

【図6】本発明の実施形態2に係る暗号通信システム全体の構成と暗号通信の原理を説明するための図である。

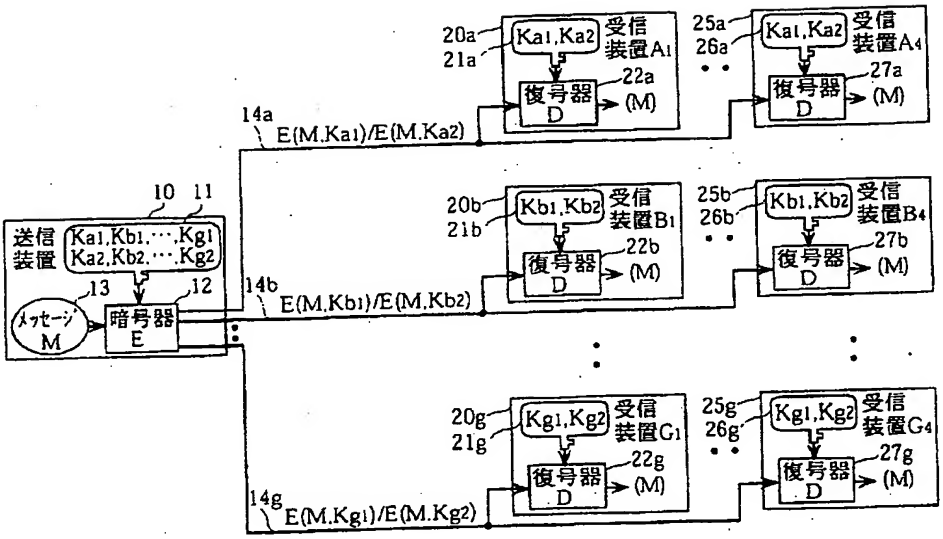
【図7】本発明の実施形態3に係る暗号化装置の構成を示すブロック図である。

【図8】同暗号化装置によって暗号化される前のブロックデータData及び暗号化された後のブロックデータEdataの構造を示す図である。

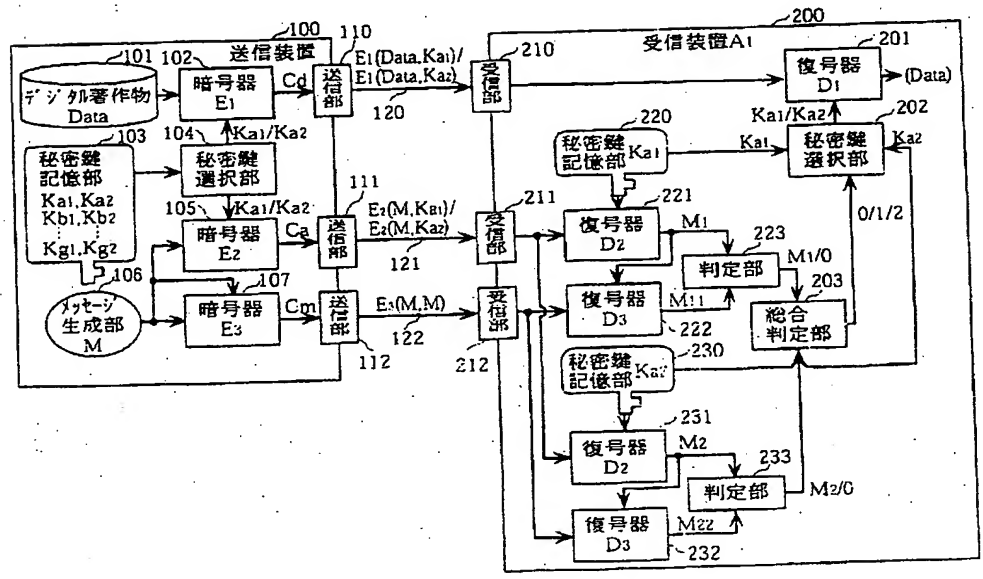
【符号の説明】

10　送信装置
11　秘密鍵
12　暗号器
13　メッセージ
14a～14g　バスライン
20a、25a　グループAの受信装置A1、A4
20b、25b　グループBの受信装置B1、B4
20g、25g　グループGの受信装置G1、G4
21a、26a　グレープA用の秘密鍵
21b、26b　グレープB用の秘密鍵
21c、26c　グレープC用の秘密鍵
22a～22g、27a～27g　復号器
100　送信装置
101　デジタル著作物
102　暗号器E1
103　秘密鍵記憶部
104　秘密鍵選択部
105　暗号器E2
106　メッセージ生成部
107　暗号器E3
110～112　送信部
120～122　バスライン
201　復号器D1
202　秘密鍵選択部
203　総合判定部
210～212　受信部
220　秘密鍵（Ka1）記憶部
221　復号器D2
222　復号器D3
223　判定部
230　秘密鍵（Ka2）記憶部
231　復号器D2
232　復号器D3
233　判定部
250　CD－ROM
251～257　記録領域
300　記録装置
301　マスター鍵記憶部
302　媒体鍵生成部
303　タイトル鍵生成部
304　デジタル著作物
305～307　暗号器E1～E3
310　DVD
311　暗号化媒体鍵
312　暗号化タイトル鍵
313　暗号化デジタル著作物
320　再生装置
321　マスター鍵記憶部
322～324　復号器D1～D3
400　暗号化装置
401　タイトル鍵生成部
402　デジタル著作物
403　修正部
404　分離部
405　暗号器E
406　結合部

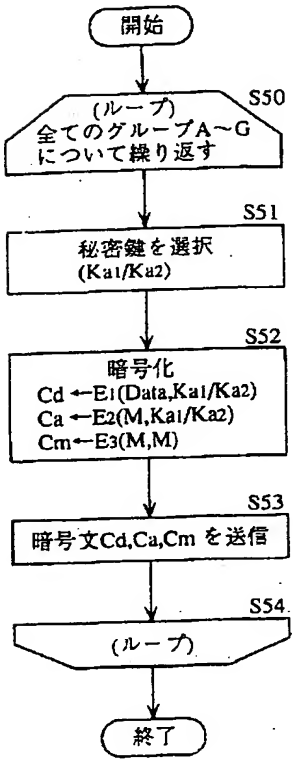
【図１】


送信装置
Ka1,Kb1,…,Kg1
Ka2,Kb2,…,Kg2
メッセージ M
暗号器 E
10 11 12 13
14a E(M,Ka1)/E(M,Ka2)
14b E(M,Kb1)/E(M,Kb2)
14g E(M,Kg1)/E(M,Kg2)
20a 21a Ka1,Ka2 受信装置A1
25a 26a Ka1,Ka2 受信装置A4
20b 21b Kb1,Kb2 受信装置B1
25b 26b Kb1,Kb2 受信装置B4
20g 21g Kg1,Kg2 受信装置G1
25g 26g Kg1,Kg2 受信装置G4
復号器 D
22a 22b 22g 27a 27b 27g (M)

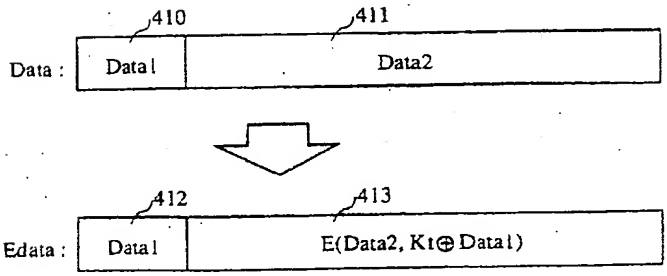
【図２】


送信装置 100
受信装置A1 200
デジタル著作物 Data 101
暗号器 E1 102
Cd
送信部 110
E1(Data,Ka1)/ E1(Data,Ka2) 120
受信部 210
復号器 D1 201
(Data)
Ka1/Ka2
秘密鍵記憶部 Ka1,Ka2 Kb1,Kb2 Kg1,Kg2 103
秘密鍵選択部 104
秘密鍵記憶部 Ka1 220
秘密鍵選択部 202
暗号器 E2 105
Ca
送信部 111
E2(M,Ka1)/ E2(M,Ka2) 121
受信部 211
復号器 D2 221
M1
判定部 223
M1/0
0/1/2
メッセージ生成部 M 106
暗号器 E3 107
Cm
送信部 112
E3(M,M) 122
受信部 212
復号器 D3 222
M11
総合判定部 203
秘密鍵記憶部 Ka2 230
復号器 D2 231
M2
判定部 233
M2/0
復号器 D3 232
M22

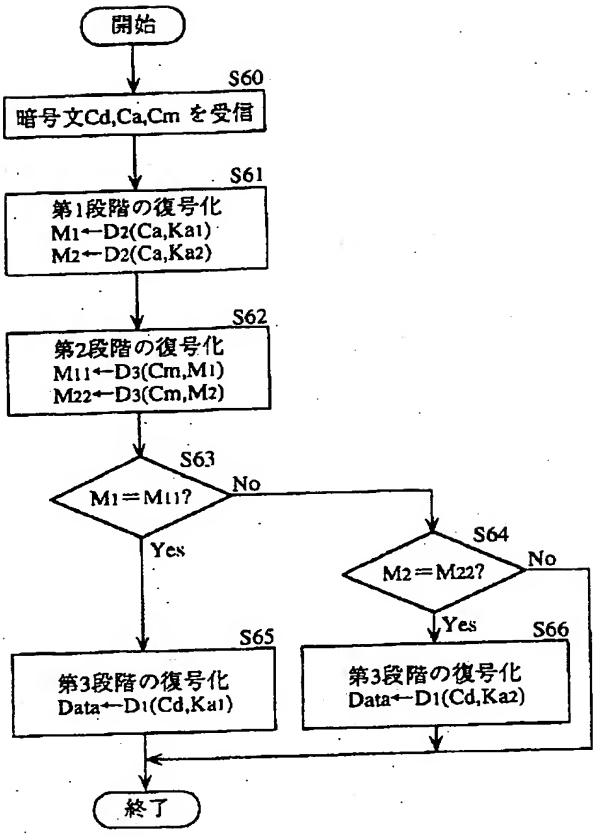
【図３】


開始
S50
(ループ) 全てのグループA～Gについて繰り返す
S51
秘密鍵を選択 (Ka1/Ka2)
S52
暗号化
Cd ←E1(Data,Ka1/Ka2)
Ca ←E2(M,Ka1/Ka2)
Cm←E3(M,M)
S53
暗号文Cd,Ca,Cm を送信
S54
(ループ)
終了

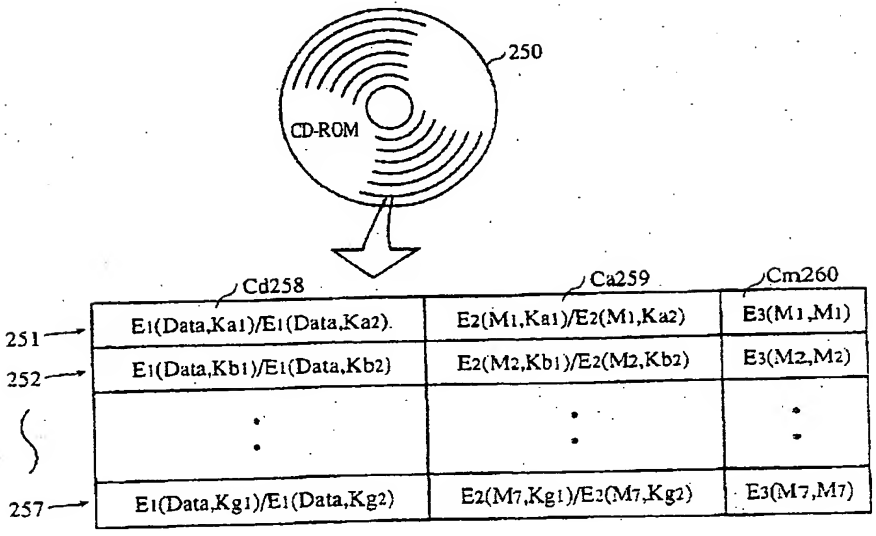
【図８】


Data :
410 Data1
411 Data2
Edata :
412 Data1
413 E(Data2, K1⊕Data1)

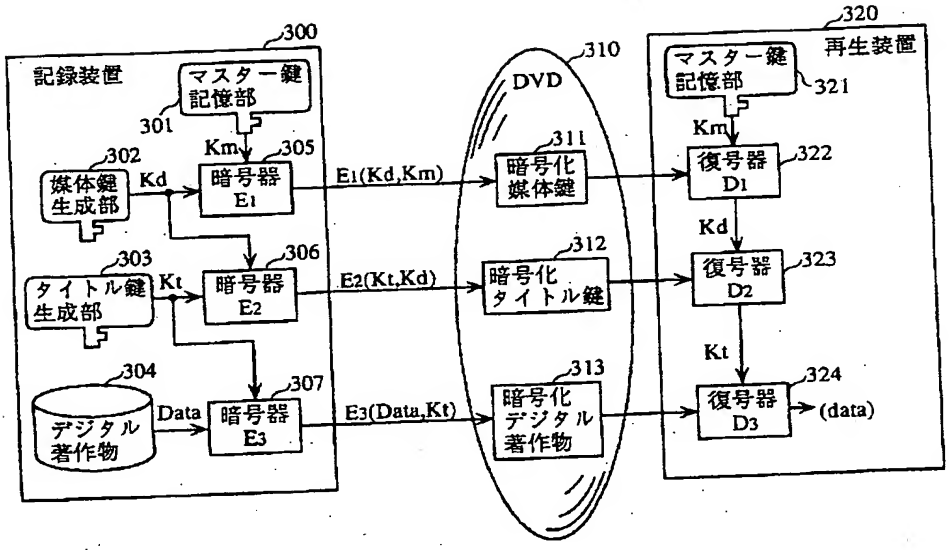
【図４】


開始
S60
暗号文Cd,Ca,Cm を受信
S61
第1段階の復号化
M1←D2(Ca,Ka1)
M2←D2(Ca,Ka2)
S62
第2段階の復号化
M11←D3(Cm,M1)
M22←D3(Cm,M2)
S63
M1＝M11?
No
Yes
S64
M2＝M22?
No
Yes
S65
第3段階の復号化
Data←D1(Cd,Ka1)
S66
第3段階の復号化
Data←D1(Cd,Ka2)
終了

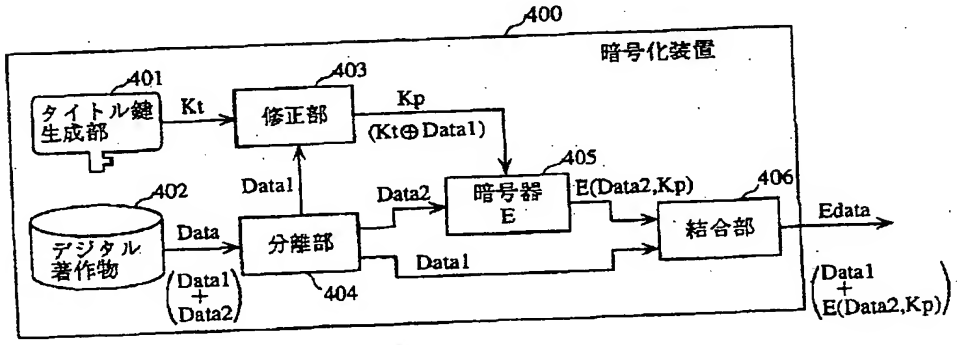
【図５】


250
CD-ROM
Cd258
Ca259
Cm260
251
252
257
E1(Data,Ka1)/E1(Data,Ka2)
E2(M1,Ka1)/E2(M1,Ka2)
E3(M1,M1)
E1(Data,Kb1)/E1(Data,Kb2)
E2(M2,Kb1)/E2(M2,Kb2)
E3(M2,M2)
E1(Data,Kg1)/E1(Data,Kg2)
E2(M7,Kg1)/E2(M7,Kg2)
E3(M7,M7)

【図6】



【図7】



フロントページの続き

(72)発明者　加藤　岳久
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　平山　康一
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内